UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v.

MARCUS A. OWENS,

Defendant.

Case No. 16-CR-38-JPS

ORDER

On March 1, 2016, a grand jury sitting in the Eastern District of Wisconsin returned a two-count indictment against Marcus A. Owens. Indictment (Docket #9). Mr. Owens is charged with one count of knowingly receiving child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and one count of knowingly possessing matter that contained images of child pornography, in violation of 18 U.S.C. § 2252A(a)(5). (Docket #9). This matter comes before the Court on Mr. Owens's motion to suppress based on the issuing magistrate judge's lack of jurisdiction to issue the initial Network Investigative Technique ("NIT") search warrant which underlies this prosecution. (Docket #40).

On October 4, 2016, Magistrate Judge David E. Jones issued a Report and Recommendation ("the Report") with this Court, recommending that the motion to suppress be denied. (Docket #63). On October 18, 2016, Mr. Owens filed written objections to the findings pursuant to 28 U.S.C. § 636(b(1)(C). (Docket #66). On October 31, 2016, the government filed a response to the objections, (Docket #75), and on November 7, 2016, Mr. Owens filed a reply (Docket #79). The objections to the Report are now fully briefed and ready for disposition. As discussed below, the Court adopts the recommendation of

Magistrate Jones and will accordingly deny Mr. Owens's motion to dismiss the indictment.

1. BACKGROUND

This case arises out a large-scale FBI investigation into a child pornography website. For the purposes of this Order, the Court presumes the parties' familiarity with the background of this case. The parties do not dispute any of the facts related to the present motion, and therefore the Court will only provide a brief overview of the facts. As discussed in detail below, numerous district courts around the country have already considered nearly the identical issues arising out of the investigation and warrants issued in this case.

In September 2014, FBI agents began investigating a website that appeared to be dedicated to the advertisement and distribution of child pornography. (Affidavit in Support of Application for NIT Warrant ("NIT Warrant Aff.") ¶ 11, Docket #39-2 at 5-37. The website, "Playpen"—referred to in the warrant applications as "Target Website" and "Website A" respectively—had more than 150,000 registered users and contained tens of thousands of posts related to child pornography. (NIT Warrant Aff. ¶¶ 10-13).

Playpen did not reside on the traditional or "open" internet. (NIT Warrant Aff. ¶ 10). Instead, Playpen operated only on the "Tor" network, an open-source software tool which routes communications through multiple computers called "nodes" in order to mask a user's IP address. Users have to download specific Tor software or utilize a Tor "gateway" to get onto the Tor network and then navigate to a site like Playpen. (NIT Warrant Aff. ¶ 7).

This process is used to keep the website user's identity anonymous. (NIT Warrant Aff. ¶¶ 7-9).

1.1 The Network Investigative Technique Warrant

In February 2015, the FBI apprehended the administrator of Playpen and took control of the website. (NIT Warrant Aff. ¶ 30). Rather than shut down Playpen, however, the FBI operated the website from a government facility in the Eastern District of Virginia for close to two weeks in an effort to identify website users. On February 20, 2015, an FBI special agent applied to a United States Magistrate Judge in the Eastern District of Virginia for a warrant to use a NIT to investigate Playpen's users and administrators. In support of the warrant application, the agent submitted a thirty-three-page affidavit that set forth his basis for probable cause to believe that deploying the NIT would uncover evidence and instrumentalities of certain child exploitation crimes. *See generally* NIT Warrant Aff.

The NIT involved additional computer instructions that would be downloaded to a user's computer—referred to as an activating computer—along with the site's normal content. NIT Warrant Aff. ¶ 33. After downloading the additional instructions, the activating computer would transmit certain information to the government-controlled computer located in the Eastern District of Virginia, including: (1) the computer's actual IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) the computer's operating system; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's "Host Name"; (6) the computer's active operating system username; and (7) the computer's "Media Access Control" address. NIT

Warrant Aff. ¶¶ 33-34, 36. The NIT would be deployed each time a user logged onto the government-controlled website. NIT Warrant Aff. ¶ 36.

On February 20, 2015, United States Magistrate Judge Theresa Carroll Buchanan, sitting in the Eastern District of Virginia, signed the NIT Warrant. (NIT Warrant, Docket #39-2 at 2-4). The face of the NIT Warrant authorized the government to search property located in the Eastern District of Virginia. (NIT Warrant at 2). Additionally, the NIT Warrant further described the property to be searched in "Attachment A" to the warrant. (NIT Warrant at 2).

Attachment A of the NIT Warrant stated that the warrant "authorize[d] the use of [an NIT] to be deployed on the computer server described below, obtaining information described in Attachment B from the activating computers described below." (NIT Warrant at 3). It explained that the computer server, which was located at a government facility in the Eastern District of Virginia, was operating a Tor network child pornography website. Further, it stated that the activating computers were those of any user or administrator who logged into the child pornography website. (NIT Warrant, Docket #39-2 at 3).

Attachment B identified the property to be seized. It listed seven pieces of information to be seized "[f]rom any 'activating' computer": (1) the IP address, and the date and time the NIT determined the IP address; (2) a unique identifier generated by the NIT; (3) the type of operating system running on the computer; (4) information about whether the NIT had already been delivered to the activating computer; (5) the activating computer's Host Name; (6) the activating computer's active operating system username; and

(7) the activating computer's media access control address. (NIT Warrant at 4).

Through the use of the NIT and additional investigation, FBI agents determined that an individual with the username "tinderbittles" registered an account on Playpen on February 3, 2015, and accessed the site for more than three hours between February 3 and March 4, 2015. (Residence Warrant Aff. ¶¶ 25-26, Docket #39-1). This user accessed several posts that contained links to and sample photos of child pornography. (Residence Warrant Aff. ¶¶ 27-31). Agents learned the user's IP address via the NIT, determined the service provider of the IP address, and linked the IP address to Mr. Owens at his home in Kenosha, Wisconsin. (Residence Warrant Aff. ¶¶ 25-34).

1.2 The Residential Warrant

With this information, an FBI agent subsequently applied for a warrant to search the Kenosha residence. In support of the warrant application, the agent submitted a thirty-four-page affidavit that set forth his basis for probable cause to believe that the residence contained evidence relating to federal violations concerning child pornography. (*See generally* Residence Warrant Aff., Docket #39-1 at 8-41). This affidavit recited much of the information contained in the NIT Warrant Affidavit. See Residence Warrant Aff. ¶¶ 7-21. United States Magistrate Judge Nancy Joseph signed the warrant on February 1, 2016. (Residence Warrant at 1, Docket #39-1).

Law enforcement officers executed the warrant on February 4, 2016, and seized—among other things—an external hard drive that contained numerous images and videos of suspected child pornography. (Criminal Complaint ¶ 5, Docket #1). Mr. Owens agreed to speak with law enforcement, and he admitted to accessing certain websites that contained

images of child pornography. (Criminal Complaint ¶ 8). Based on the evidence seized from the residence and his statement to law enforcement, Mr. Owens was arrested pursuant to a criminal complaint that charged him with receiving and possessing child pornography. (*See* Criminal Complaint).

On March 1, 2016, a grand jury indicted Mr. Owens for one count of knowingly receiving child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and one count of knowingly possessing matter that contained images of child pornography, in violation of 18 U.S.C. § 2252A(a)(5). (Indictment, Docket #9).

2. LEGAL STANDARD

Pursuant to 28 U.S.C. § 636(b)(1)(B), a magistrate judge may consider potentially dispositive motions, such as a motion to dismiss, and issue proposed recommendations to the district judge regarding the motion. When reviewing a magistrate's recommendation, the Court is obliged to analyze the portions of the report to which the defendant has lodged objections *de novo*. 28 U.S.C. § 636(b)(1)(C). Thus, the Court can "accept, reject, or modify, in whole or in part, the findings or recommendations made by the magistrate." *Id.* In other words, the Court's *de novo* review of Magistrate Jones's Report is not limited to his legal analysis alone; rather, the Court may also review the factual findings and accept, reject, or modify those findings as it sees fit based upon the evidence. *Id.*

3. DISCUSSION

Mr. Owens seeks to suppress all evidence seized from his computer through the NIT search, as well as the fruits of that search. The Report recommends denying the motion to suppress based on the issuing magistrate's lack of jurisdiction. Mr. Owens objects to the recommendation

and argues, among other things, that: (1) the NIT Warrant was invalid; (2); the good faith exception should categorically not apply to warrants issued without jurisdiction, and (3) regardless, there was no good faith in this case. Mr. Owens heavily relies on the reasoning of several district courts around the country that have granted similar motions to dismiss on this exact issue. While the Court finds Mr. Owens's argument and the reasoning of these district court decisions to be quite persuasive, it nonetheless finds that Seventh Circuit precedent dictates denying the motion to suppress. For the reasons discussed below, the Court agrees with Judge Jones's recommendation, although for slightly different reasons, and will therefore deny the motion to suppress based on the issuing magistrate judge's lack of jurisdiction.

3.1 Fourth Amendment Applicability

The Court begins its analysis with a brief discussion on the threshold issue of whether Mr. Owens had a reasonable expectation of privacy in the things and places searched. Although the parties spend little time on this issue, the Court finds it important to address before proceeding any further. If Mr. Owens had no reasonable expectation of privacy in the places or things searched, then the Fourth Amendment would not apply and the Court could end its discussion.

A Fourth Amendment search occurs when "the government violates [the defendant's] subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001); *see Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). And "[a]lthough it has become an old saw that the Fourth Amendment protects people, not places, the starting point in the *Katz* inquiry generally 'requires reference to a

place.'" *United States v. Cuevas–Perez*, 640 F.3d 272 (7th Cir. 2011) (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (internal quotation marks omitted)). In 2010, the Seventh Circuit reiterated its reliance on a five-factor test, originally announced in *United States v. Peters*, 791 F.2d 1270 (7th Cir.1986), used to determine whether a defendant had such a privacy interest:

> (1) whether the defendant had a possessory [or ownership] interest in the thing seized or the place searched, (2) whether he had the right to exclude others from that place, (3) whether he exhibited a subjective expectation that it would remain free from governmental invasion, (4) whether he took normal precautions to maintain his privacy, and (5) whether he was legitimately on the premises.

United States v. Carlisle, 614 F.3d 750, 758 (7th Cir. 2010) (citing *Peters*, 791 F.2d at 1281).

The government focuses on Mr. Owen's expectation of privacy in his IP address, (Docket #75 at 13 n.5), whereas Mr. Owens focuses on his expectation of privacy in the contents of his computer (Docket #66 at 14). While some courts have only addressed the expectation of privacy in the IP address, the Court finds the question to be two-fold. *See United States v. Broy*, — F. Supp. 3d —, No. 16-CR-10030, 2016 WL 5172853, at *4 (C.D. Ill. Sept. 21, 2016 ("Whether Broy had a reasonable expectation of privacy in his computer and its contents is equally as important as whether he had one in his IP address."). As such, the Court will address each argument in turn.

3.1.1 Privacy in IP Address

The Seventh Circuit recently addressed the issue of whether a person has a reasonable expectation of privacy in his or her IP address in *United States v. Caira*, 833 F.3d 803 (7th Cir. 2016). There, the DEA subpoenaed

Microsoft Corporation (the owner of Hotmail), asking for basic information including, among other things, the user's "IP Login history," which the user had necessarily and voluntarily communicated to both Microsoft and Comcast Corporation (the owner of the IP address commonly associated with the email account). *Id.* at 805. The court held that sharing his IP address with a third party negated the defendant's reasonable expectation of privacy for Fourth Amendment purposes. *Id.* at 806. The court further noted that even if the defendant had a subjective expectation of privacy in such information, "once information is voluntarily disclosed to a third party, any such expectation is 'not one that society is prepared to recognize as reasonable.'" *Id.* (quoting *Smith v. Maryland*, 442 U.S. 735, 743 (1979)).

Similarly, Mr. Owens likely had a subjective expectation of privacy in his IP address due to the fact he was using the Tor network to conceal his identity. However, under *Caira*, Mr. Owens lost that expectation of privacy when he voluntarily disclosed his IP address to the operator of the first Tor node, a third party. As such, the Court is obliged to find that Mr. Owens had no reasonable expectation of privacy in his IP address. The Court now turns to the question of whether Mr. Owens's had a reasonable expectation of privacy in his computer.

3.1.2 Privacy in Computer

The Court agrees with Mr. Owens that he had a reasonable expectation of privacy in the contents of his computer. One court eloquently described why the focus should be on the expectation of privacy in the computer as opposed to the IP address:

> The NIT searches the user's computer to discover the IP address associated with that device. Therefore, one's expectation of privacy in that device is the proper focus of the

> analysis, not one's expectation of privacy in the IP address residing in that device. For example, a defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage. Remove the stolen car from the garage, and no expectation of privacy in the vehicle exists. An IP address located in the "open" is akin to a stolen car parked on the street. However, the agents were required to deploy the NIT to search the contents of Defendant's laptop, and Defendant enjoyed a reasonable expectation of privacy in that device.

Adams, 2016 WL 4212079 at *4.

In looking to the five-factor test, the Court finds that all factors weigh in Mr Owens's favor of a reasonable expectation of privacy. The record shows that Mr. Owens owned the computer and therefore had a possessory interest in it, he likely had a subjective expectation of privacy based on his use of the Tor network to conceal his identity, and he was legitimately on his own computer in his residence. As such, the Court finds that the use of the NIT constituted a Fourth Amendment search.[1] In light of this conclusion, the Court turns its attention to the issue of whether the warrant upon which the search was premised was valid.

3.2 Validity of NIT Warrant

3.2.1 Federal Magistrate Act and Rule 41

---

[1]Various district courts have already addressed this issue in relation to the specific NIT Warrant in this case. The Court agrees with the majority of courts finding a Fourth Amendment search occurred. *See Broy*, 2016 WL 5172853, at *6; *United States v. Ryan Anthony Adams*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016); Darby, —— F. Supp. 3d at —— – ——, 2016 WL 3189703 at **5–6; *but see United States v. Matish*, No. 4:16CR16, —— F. Supp. 3d ——, 2016 WL 3545776 at *22 (E.D. Va. June 23, 2016) (finding no Fourth Amendment search because "the NIT only obtained identifying information; it did not cross the line between collecting addressing information and gathering the contents of any suspect's computer").

In support of his motion to suppress, Mr. Owens argues that the NIT Warrant does not comply with the territorial restrictions of Federal Rule of Criminal Procedure 41(b) and that the issuing magistrate judge lacked jurisdiction to authorize the warrant under the Federal Magistrates Act, 28 U.S.C. § 636(a).[2]

Magistrate judges are creatures of federal statute that have specific, delineated powers. *See* 28 U.S.C. § 636(a). The Federal Magistrates Act provides magistrate judges a list of powers and limits where they can exercise those powers. Section 636(a) provides, in relevant part, as follows:

> (a) Each United States magistrate judge . . . shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law—
>
> (1) all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure.

28 U.S.C. § 636(a). Because the Federal Magistrate Act specifically incorporates the Federal Rules of Criminal Procedure, the Court looks to them for guidance as to a magistrate judge's authority to issue a warrant. Rule 41(b) of the Federal Rules of Criminal Procedure—titled "Authority to Issue a Warrant" provides magistrate judges power to issue warrants.

"Rule 41(b) sets out five alternative territorial limits on a magistrate judge's authority to issue a warrant." *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 756 (S.D. Tex. 2013). Specifically, Rule 41(b) authorizes magistrate judges to issue warrants to: (1) "search for and seize a person or property located within [the judge's] district"; (2)

[2]The Court will refer to Federal Rule of Criminal Procedure 41 as simply "Rule 41" for the remainder of this Order.

search for and seize a person or property located outside the judge's district "if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed"; (3) search for and seize a person or property located outside the judge's district if the investigation relates to terrorism; (4) "install within [the judge's] district a tracking device . . . to track the movement of a person or property located within the district, outside the district, or both; or (5) seize property located outside the judge's district but within a United States territory, possession, commonwealth, or premises used by a United States diplomatic or consular mission. Fed. R. Crim. P. 41(b). The Court now turns to the question of whether the magistrate judge who issued the NIT Warrant complied with Rule 41(b).

3.2.2 NIT Warrant Violates Rule 41(b)

The Report noted it was skeptical whether the NIT Warrant complied with the territorial restrictions of Rule 41(b), but did not ultimately decide the issue. (Docket #63 at 8-9), The Court parts ways with the Report in this regard and joins the majority of courts who have definitively found the NIT Warrant did not comply with Rule 41(b). *See Broy*, 2016 WL 5172853, at *8; *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016); *United States v. Werdene*, No. CR 15-434, 2016 WL 3002376, at *7 (E.D. Pa. May 18, 2016); *Adams*, 2016 WL 4212079, at *6; *United States v. Acevedo-Lemus*, No. SACR 15-00137-CJC, 2016 WL 4208436, at *8 (C.D. Cal. Aug. 8, 2016) ; *United States v. Torres*, Case No. 5:16-CR-285, 2016 WL 4821223, at *7 (W.D. Tex. Sept. 9, 2016); *United States v. Ammons*, Case No. 3:16-CR-00011, 2016 WL 4926438, at *7 (W.D. Ky. Sept. 14, 2016); *United States v. Henderson*, Case No. 15-CR-00565, 2016 WL 4549108, at *4 (N.D. Cal. Sept.

1, 2016); *Anzalone*, 2016 WL 5339723, at *9); *United States v. Allain*, Case No. 15-CR-10251, 2016 WL 5660452, at *11 (D. Mass. Sept. 29, 2016); *United States v. Scarbrough*, Case No. 3:16-CR-035, 2016 WL 5900152, at *2 (E.D. Tenn. Oct. 11, 2016); *but see Darby*, 2016 WL 3189703, at *11 ("It is understandable why the government sought the warrant in the Eastern District of Virginia. The government planned to run the website from a server located in the district. No district in the country had a stronger connection to the proposed search than this district. Additionally, nothing in Rule 41 categorically forbids magistrates from issuing warrants that authorize searches in other districts—most of its provisions do just that.").

Here, none of the five jurisdictional allowances in Rule 41(b) apply. At all relevant times, Mr. Owen's computer was located in Wisconsin, and therefore it was not located in the Eastern District of Virginia, as it must be for the magistrate judge to have the authority to issue the warrant under Rule 41(b)(1) or 41(b)(2). Further, there was no form of terrorism involved to invoke Rule 41(b)(3), the NIT was not a tracking device under Rule 41(b)(4), and the computer was located in Wisconsin and not a United States territory, possession, or commonwealth owned by the government to invoke Rule 41(b)(5).[3]

In addition to a majority of courts finding a violation of Rule 41, a recently proposed amendment to Rule 41(b) strongly suggests the NIT

[3]The Court recognized that various arguments have been made in relation to whether the NIT warrant should be considered a tracking device under Rule 41(b)(4). Under most circumstances, the Court would more thoroughly address these arguments in full, however, in this case it makes no difference to the Court's ultimate conclusion. As such, the Court feels it unnecessary to address the issue further.

Warrant was not authorized in this case. On April 28, 2016, the Supreme Court submitted the following proposed amendment to Rule 41(b) to the Congress:

> (b) at the request of a federal law enforcement officer or an attorney for the government ...
>
> > (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
> >
> > > (A) the district where the media or information is located has been concealed through technological means; or ...

Letter from Justice John G. Roberts to the Honorable Paul D. Ryan and the Honorable Joseph R. Biden, Jr. (Apr. 28, 2016), www.uscourts.gov/file/19848/download. This proposed amendment, if adopted, will directly address the issue before the Court today. In light of the proposed amendment and the plain language of Rule 41(b), the Court concludes that the magistrate judge issued the NIT Warrant without jurisdiction, in violation of Rule 41(b).

In light of the Rule 41(b) violation, the Court concludes that the NIT search occurred without a valid warrant. *See Cazares-Olivas*, 515 F.3d 726, 728 (7th Cir. 2008) (finding the search occurred "without a warrant" upon finding Rule 41 violation); *Broy*, 2016 WL at *8 (finding that warrant issued without lawful authority under Rule 41(b) was "void at the outset, or *ab initio*"). Upon

finding the NIT search occurred without a warrant, the only question remaining is whether suppression is appropriate in this instance.[4]

3.3 Is Suppression of Evidence the Appropriate Remedy?

"The fact that a Fourth Amendment violation occurred...does not necessarily mean that the exclusionary rule applies." *Herring v. United States,* 555 U.S. 135, 140 (2009). Here, Mr. Owens argues that: (1) the good faith exception should not apply, categorically, to warrants issued without jurisdiction; and (2) even if the good faith exception could apply, there was no good faith in this case. (Docket #66 at 16-18).

Before beginning his argument, Mr. Owens specifically acknowledges Seventh Circuit precedent that holds violations of the federal rules of criminal procedure categorically do not warrant the suppression of evidence. (Docket #66 at 8); *see also Cazares-Olivas,* 515 F.3d at 730 (stating unequiviocally that "[v]iolations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probably cause, and with advance judicial approval"); *United States v. Trost,* 152 F.3d 715, 722 (7th Cir. 1998) ("[I]t is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the fourth amendment, that wuld call for suppression."). Mr Owens maintains, however, that the Rule 41 violation

---

[4]The Court notes that its conclusion here differs again from the Report. The Report found that a "warrant issued without jurisdiction...falls somewhere between a defective warrant and no warrant at all." (Docket #63 at 14) (citing *United States v. Baker*, 894 F.2d 1144, 1147 (10th Cir. 1990). The Court agrees with Mr. Owens that *Baker* does not reach that conclusion; in contrast, *Baker* found the warrant issued without jurisdiction to be invalid. *Baker,* 894 F.3d at 1147-49 ("[W]e hold that the search of defendant's property was not authorized by a valid warrant."). The *Baker* court later discussed the attributes of a warrant issued without jurisdiction in the context of whether it could apply the good faith exception in that context. *See id.*

in this case is different here because the magistrate judge acted without jurisdiction to issue the NIT Warrant. (Docket #66 at 8).

3.3.1 Does the Good Faith Exception Apply?

Mr. Owens maintains that the good faith exception should categorically not apply to warrants issued without jurisdiction. Owens relies heavily on the reasoning of *United States v. Levin*, Case No.15-CR-10271, 2016 WL 2596010 (D. Mass. May 5, 2016), and *United States v. Workman*, No. 15-CV-00397-RBJ-1, 2016 WL 5791209, at *7-*8 (D. Colo. Sept. 6, 2016) that recently concluded the good faith exception does not apply to warrants issued without jurisdiction. (Docket #66 at 16-17). On their face, the reasoning of these decisions is persuasive. Mr. Owen's argument fails, however, to convincingly distinguish this case from Seventh Circuit precedent finding that a Rule 41(b) violation does not invoke the exclusionary rule.

In *United States v. Berkos,* 543 F.3d 392, 396 (7th Cir. 2008), the Seventh Circuit was confronted with a similar Rule 41(b) violation. There, a magistrate judge in the Northern District of Illinois authorized a search warrant for an out-of-district internet service provider located in the Southern District of Texas. *Id.* The court noted that this question inadvertently presented the question of "whether a violation of Federal Rule of Criminal Procedure 41(b), which discusses authority to issue search warrants, merits invoking the exclusionary rule." *Id.* In other words, does the exclusionary rule apply to evidence seized if the warrant was issued without jurisdiction? The court reiterated the longstanding Seventh Circuit principle that "'violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause and with advance judicial approval.'" *Id.* (quoting *Cazares–Olivas*, 515 F.3d at 730).

The court then held that this principle "alone merits affirming the district court's denial of [the] first motion to suppress." *Id.* The court further remarked that the remedy of allowing a defendant to go free based on a violation of Rule 41's requirements would be "wildly out of proportion to the wrong." *Id*. (quoting *Cazares-Olivas*, 515 F.3d at 730). Although the court did not expressly state it, this conclusion strongly suggests that a Rule 41(b) violation—a warrant issued without jurisdiction—would never trigger the exclusionary rule. The court's analysis, however, was fairly limited because the parties did not raise the Rule 41(b) issue, and so the court found it best to decided the issue on the merits.

Similarly, in *Cazares–Olivas*, the Seventh Circuit found a search occurred "without a warrant" because the magistrate judge failed to comply with the requirements of Rule 41(e) for a telephonic warrant. 515 F.3d at 728. In finding a Fourth Amendment violation, the court turned to the question of whether the exclusionary rule should apply, and concluded it did not. *Id.* at 728-29. The court reasoned that the defendants "received the benefit of a magistrate judge's impartial evaluation...[,t]he search was supported by probable cause—on a record fixed, and supported by an oath, in advance, to prevent hindsight from being invoked to justify the search." *Id.* at 729.

Here, the Court is confronted here with nearly the identical situation as *Berkos*—namely, whether a Rule 41(b) violation merits invoking the exclusionary rule. *Berkos*, at 396. Notably, Mr. Owens's objections to the Report fail to even mention, much less convincingly distinguish, this case from *Berkos.* This failure is detrimental to Mr Owens's argument. The Court recognizes that the depth of the analysis in *Berkos* was limited, and made no specific mention of a warrant void *ab initio* or the good faith exception for

that matter. However, the warrant in *Berkos* is directly comparable to the warrant in this case; the magistrate judges both lacked jurisdiction to issue the warrant, violating Rule 41(b), and the warrants were not valid upon issuance. The Seventh Circuit made it clear that the Rule 41(b) violation in that case—a warrant by a magistrate judge without jurisdiction to issue the warrant— would not invoke the exclusionary rule and required denial of the motion to suppress. *Berkos*, 543 F.3d at 396. Thus, in light of *Berkos*, the Court is obliged to find that the exclusionary rule does not apply to the Rule 41(b) violation in this case.[5] As such, the Court will adopt Magistrate Jones's recommendation and will deny Mr. Owen's motion to suppress the evidence based on the issuing magistrate judge's lack of jurisdiction.

4. CONCLUSION

In sum, the Court agrees with the ultimate conclusion of Magistrate Jones and finds that suppression of the evidence is not warranted in this case. Although a the magistrate judge violated Rule 41(b) by issuing the NIT Warrant without jurisdiction, Seventh Circuit precedent indicates the exclusionary rule does not apply in this circumstance. Thus, the Court will

---

[5] *Berkos* contained no discussion of whether the good faith exception should apply to the Rule 41(b) violation, and instead simply held the exclusionary rule did not apply to the Rule 41(b) violation. The Court notes, however, that if it were to apply the exception here, the Court would find good faith. A defendant can rebut the presumption of good faith by showing that: (1) the issuing judge abandoned his role as a neutral and detached arbiter; (2) the officers were reckless or dishonest in preparing the supporting affidavit; or (3) the affidavit was so lacking in probable cause that no officer could have reasonably relied on it. *United States v. Mykytiuk*, 402 F.3d 773, 777 (7th Cir. 2005) (citing Leon, 468 U.S. at 923). Here, there is no indication that the judge abandoned her neutral role, no support in the record that the officers were reckless or dishonest in preparing the affidavit, and, as discussed in a related order, sufficient probable cause existed to reasonably rely on the NIT Warrant.

adopt the Report and deny Mr. Owens's motion to suppress the evidence based on the issuing magistrate's lack of jurisdiction.

Accordingly,

IT IS ORDERED that Magistrate Judge David E. Jones's report and recommendation (Docket #63) be and the same is hereby **ADOPTED**;

IT IS FURTHER ORDERED that, consistent with the Court's adoption of the report and recommendation, Mr. Owens's motion to suppress (Docket #40) be and the same is hereby **DENIED**.

Dated at Milwaukee, Wisconsin, this 5th day of December, 2016.

BY THE COURT:

s/ *J. P. Stadtmueller*
J.P. Stadtmueller
U.S. District Judge